UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,277	10/28/2003	Yong Ho Son	SEDN/152CON2	3963

56015 7590 05/14/2008
PATTERSON & SHERIDAN, LLP/
SEDNA PATENT SERVICES, LLC
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
SAINT CYR, JEAN D	

ART UNIT	PAPER NUMBER
2623	

MAIL DATE	DELIVERY MODE
05/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/695,277	**Applicant(s)** SON ET AL.	
	Examiner JEAN D. SAINT CYR	**Art Unit** 2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *three*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/28/2003* is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. **Response to Amendment**

This action is in response to applicant's amendment filed on 04/23/2008.

Claims 1-11 are still pending in the present application. **This action is made NON-FINAL**.

Response to Arguments

Applicant's arguments filed on 04/23/2008 have been totally considered. As mentioned in the first office action, claims 1-9 of the current are similar to claims 1-9 of the US. Patent 6681326. The difference between these two sets of claims is not significant. In the current application, the applicant only added remote server just to show that the claims of the current application are different from the claims of the US. Patent 6681326.

Applicant argues that Heer et al did not disclose partially and fully encrypted program. However, the examiner found in updating his search that Kupka et al disclose If the digital content to be download is stored on the server 16 in an encrypted format , pre-encrypted, prior to downloading then the server would need only encrypt the data key to the content ,i.e., the software application, music or video. Pre-encryption may be preferable to provide greater performance in environments where large amounts of data need to be encrypted per transaction, col.19, lines 2-9; however, it may be preferable to double encrypt the downloaded content at step 308 by encrypting the pre-encrypted content and the data key to the pre-encrypted content using the unique serial identifier, col.19, lines 12-16.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re*

Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

Claims 1-9 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9 of US. Patent No. 6681326. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1-9 are obvious variants and encompassed by claims 1-9 of the US. Patent 6681326. In order to store, process and cause transmission, we need to have a storage unit located somewhere in the system and that proves that any server that is located inside or remotely from the distribution system is not new to the system. As a result, applicant's arguments are not persuasive for the double patenting

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) The invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3 and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Kupka et al, US Patent No.6434535.

Re claim 1, Kupka et al disclose at least one programming source for storing at least one partially encrypted video program(see fig.1, server 16c; It is further noted that the E-commerce server 16c may store digital content to be downloaded in an encrypted or unencrypted format, col.18, lines 64-66); a distribution center comprising a remote server(see fig.1, server 16; present invention provides for a secure method of transmitting electronic data (content) from a remote server 16 to a removable storage media , col.7, lines 31-33), said remote server storing said at least one partially encrypted video program(It is further noted that the E-commerce server 16c may store digital content to be downloaded in an encrypted or unencrypted format, col.18, lines 64-66)received from said at least one programming source(see fig.1, server 16), and said remote server processing (the electronic data is encrypted during the download process to the media 28 using the unique identifier of the media 28, a vendor identifier and a user identifier as an encryption key, col.14, lines 35-38)said partially encrypted video program corresponding to a subscriber requested(user initiates the electronic data distribution process at step 300 when he or she desires to purchase software, music or videos, col.13, lines 19-21; that means request from the user) video program to produce a fully encrypted video program(If the digital content to be download is stored on the server 16 in an encrypted format , pre-encrypted, prior to downloading then the server would need only encrypt the data key to the content ,i.e., the software application, music or video. Pre-encryption may be preferable to provide greater performance in environments where large amounts of data need to be encrypted per transaction, col.19, lines 2-9; however, it may be preferable to double encrypt the downloaded content at step 308 by encrypting the pre-encrypted content and the data key to the pre-encrypted content using the unique serial identifier, col.19, lines 12-16); and a subscriber-side distribution network coupled to the distribution center(see fig.1, element 12, network infrastructure/internet), for causing transmission of the fully encrypted video program to the requesting subscriber(however, it may be preferable to double encrypt the downloaded content at step 308 by encrypting the pre-encrypted content and the data key to the pre-encrypted content using the unique serial identifier, col.19, lines 12-16).

Re claim 2, Kupka et al disclose wherein said remote server causes transmission of a decryption key to said requesting subscriber via said subscriber-side distribution network, said decryption key being necessary to decrypt said fully encrypted video program(see fig.6, step 228, send authorization key to client; the electronic content may be written to the one piece of destination media in an encrypted format using the compound key as a decryption key, col.5, lines 2-5).

Re claim 3, Kupka et al disclose wherein said fully encrypted video program is encrypted according to a public key associated (the encrypting using the unique identifier as an encryption key, col.4, lines 34-35) with said requesting subscriber, said public key having associated with it a private key necessary to decrypt said fully encrypted video program(the data is stored on the media 28 in an encrypted format using at least the unique serial number as a decryption key, col.18, lines 46-48).

Re claim 11, Kupka et al teach wherein said distribution center is coupled to said at least one programming source via a provider side distribution network(see fig.1, server 16a and server 16c).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4-9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kupka et al in view of Heer et al, US Patent No. 5999629.

Re claim 4 , Kupka et al did not fully disclose wherein said fully encrypted video program is encrypted according to a private key associated with said requesting subscriber, said private key having associated with it a public key necessary to decrypt said fully encrypted video program.

In an analogous art, Heer et al disclose wherein said fully encrypted video program is encrypted according to a private key associated(private key, col.4, line 34) with said requesting subscriber, said private key having associated with it a public key (an associated public key, col.1, line 52) necessary to decrypt said fully encrypted video program(to decrypt the encrypted program, col.4, line 7).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce wherein said fully encrypted video program is encrypted according to a private key associated with said requesting subscriber, said private key having associated with it a public key necessary to decrypt said fully encrypted video program into the system of Kupka, as taught by Heer, for the benefit of making the system safer.

Re claim 5, Kupka et al did not explicitly disclose wherein said fully encrypted video program is encrypted according to a public key, said public key having associated with it a private key necessary to decrypt said fully encrypted video program, said apparatus further comprising: said remote server transmitting said private key to said requesting subscriber.

In an analogous art, Heer et al disclose wherein said fully encrypted video program is encrypted according to a public key(an associated public key, col.1, line 52), said public key having associated with it a private key necessary to decrypt said fully encrypted video program(to decrypt the encrypted program, col.4, line 7), said apparatus further comprising: said remote server transmitting said private key to said requesting subscriber(distribute that key in a secure manner to user who has entered a request, col.4,lines 23-24).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce wherein said fully encrypted video program is encrypted according to a public key, said public key having associated with it a private key necessary to decrypt said fully encrypted video program, said apparatus further comprising: said remote server transmitting said private key to said requesting subscriber into the system of Kupka, as taught by Heer, for the benefit of making the system safer.

Re claim 6, Kupka et al did not explicitly disclose said public key is encrypted prior to transmission to said requesting subscriber.

In an analogous art, Heer et al disclose said public key(an associated public key, col.1, line 52) is encrypted prior to transmission to said requesting subscriber(encrypted and stored in server in association of program identifier, col.2, line 63; that means public key was encrypted prior any transmission).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce said public key is encrypted prior to transmission to said requesting subscriber into the system of Kupka, as taught by Heer, for the benefit of making the system safer to unauthorized users.

Re claim 7, Kupka et al did not explicitly disclose wherein said fully encrypted video program is transmitted to said requesting subscriber via a first communications channel and said decryption key is transmitted to said requesting subscriber via a second communications channel.

In an analogous art, Heer et al disclose wherein said fully encrypted video program is transmitted to said requesting subscriber via a first communications channel and said decryption key is transmitted to said requesting subscriber via a second communications channel(see fig.1, the system uses bus 41 for encrypted video program and bus 61 for sharing key; col.6, lines 17-24; to this end, then, ACS 40 and module 30 communicate with one another via processor 25 and a communications channel of path 21 reserved for such communications to transport the "key" to ACS 40, col.4, lines 27-30; that means use a second path for channel communication).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce disclose wherein said fully encrypted video program is transmitted to said requesting subscriber via a first communications channel and said decryption key is transmitted to said requesting subscriber via a second communications channel into the system of Kupka, as taught by Heer, for the benefit of limiting congestion of bandwidth.

Re claim 8, Kupka et al did not explicitly disclose wherein said fully encrypted video program is encrypted according to a Data Encryption Standard .

In an analogous art, Heer et al disclose wherein said fully encrypted video program is encrypted according to a Data Encryption Standard (Digital Encryption System, col. 8, line 67).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce wherein said fully encrypted video program is encrypted according to a Data Encryption Standard into the system of Kupka, as taught by Heer, for the benefit of making the system more compatible.

Re claim 9, Kupka et al did explicitly disclose wherein said remote server multiplexes said fully encrypted video program and other signals to create a multiplexed signal for transmission to said requesting subscriber.

In an analogous art, Heer et al disclose wherein said remote server multiplexes said fully encrypted video program and other signals to create a multiplexed signal (see fig.5, element 7, DES processor; input data handler 6 includes an input register file configured as a FIFO, register, byte counters and a multibit, e.g., 32 bit, multiplexer, col.9. lines 63-65) for transmission to said requesting subscriber(distribute that key in a secure manner to user who has entered a request, col.4,lines 23-24).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to introduce wherein said remote server multiplexes said fully encrypted video program and other signals to create a multiplexed signal for transmission to said requesting subscriber into the system of Kupka, as taught by Heer, for the benefit of making the system more efficient.

5. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kupka et al in view of Garmeau et al, US Patent No. 5675647.

Re claim 10, Kupka et al did not explicitly disclose wherein said at least one programming source comprises at least one of a television broadcasting source, a premium broadcast source, and a video- on-demand source.

In an analogous art, Garmeau et al teach wherein said at least one programming source comprises at least one of a television broadcasting source, a premium broadcast source, and a video- on-demand source(see fig.3 where a plurality of programming sources are connected to the Headend; pay per view or equivalent service, col.1, lines 51-52).

In view of the teaching of Garmeau, it would have been obvious for any person of ordinary skill in the art at that time the invention was made to implement wherein said at least one programming source comprises at least one of a television broadcasting source, a premium broadcast source, and a video- on-demand source into the system of Kupka for the benefit of making the system more usable.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jean Duclos Saintcyr whose phone number is 571-270-3224. The examiner can normally reach on M-F 7:30-5:00 PM EST.If attempts to reach the examiner by

telephone are not successful, his supervisor, Brian Pendleton, can be reach on 571-272-7527. The fax number for the organization where the application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Retrieval (PAIR) system. Status information for published applications may be obtained from either private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see htpp://pair-direct.uspto.gov. Should you have questions on access to the private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197(toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, dial 800-786-9199(IN USA OR CANADA) or 571-272-1000.

Jean Duclos Saintcyr
05/05/2008
/Brian T. Pendleton/
Supervisory Patent Examiner, Art Unit 2623